UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ALEXANDRA PHELPS, individually, and on behalf of all others similarly situated, Plaintiff, v. ILLINOIS BONE AND JOINT INSTITUTE, LLC, Defendant.	Case No.: 1:24-cv-8555 Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff ALEXANDRA PHELPS ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), brings this Class Action Complaint ("Complaint") against Defendant ILLINOIS BONE AND JOINT INSTITUTE, LLC ("IBJI" or "Defendant"), to obtain damages, restitution, injunctive relief, and all other relief afforded by law or equity. Plaintiff makes the following allegations upon information and belief, her own personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

INTRODUCTION

1. IBJI solicited, collected, digitized, aggregated, stored, and failed and refused to protect approximately 182,670 of its patients' sensitive personally identifiable and health information from known cyber threats, including their name, address, date of birth, Social Security number, driver's license number, medical treatment or diagnosis information, and health insurance or claims information ("PII/PHI"). IBJI failed to comply with regulatory, ethical, and industry standards for cybersecurity and confidentiality of patient records, failed to take the most basic

security measures such as encryption of data and destruction of obsolete data, and failed to prevent, detect, and adequately respond to a foreseeable data breach carried out by cyber criminals. As a result, criminals gained access to, copied, and stole Plaintiff's and Class members' PII/PHI (the "Data Breach").

2. IBJI failed to prevent and detect the Data Breach. The criminal hackers gained access to IBJI's computer network on or about May 30, 2024, and remained there undetected until July 4, 2024, at which point IBJI "detected unauthorized access to certain computer systems on the IBJI network."[1]

3. Although IBJI learned of the Data Breach on July 4, 2024, it unreasonably delayed notifying Plaintiff and Class members for 57 days, giving the criminals a nearly two-month head start to commit identity fraud, theft, and wreak havoc to Plaintiff's and Class members' personal finances, identities, and accounts.

4. After an unreasonably long silence, on August 30, 2024, IBJI sent a letter to Plaintiff and Class members notifying them of the Data Breach. *See*, redacted copy of letter sent by IBJI to Plaintiff, attached hereto as Exhibit A. The letter begins by explaining that IBJI "values and respects the privacy" of Plaintiff's information, but in the second paragraph states, "On July 4, 2024, we detected unauthorized access to certain computer systems on the IBJI network." *Id*. The letter also states further down that "we have since determined that the systems may contain personal information that included" Plaintiff's "name, address, date of birth, Social Security number, medical treatment or diagnosis information, and health insurance or claims information." *Id*.

[1] https://www.ibji.com/data-security-incident/.

5. As a direct result of the Data Breach, Plaintiff and Class members have suffered numerous actual and concrete injuries and will suffer additional injuries into the future. Plaintiff seeks damages and other legal and equitable relief for the following categories of harms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in Defendant's notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) failure to receive the benefit of the bargain when IBJI failed to provide adequate and reasonable protection that caused the Data Breach; (i) deprivation of value of PII/PHI; and (j) statutory damages.

6. Plaintiff brings this class action against IBJI for IBJI's negligence, negligence *per se*, breach of implied contract, violation of the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*., and unjust enrichment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

7. Plaintiff is a natural person and a citizen of Tennessee with a residence in Davidson County, Tennessee.

8. Defendant is a limited liability company organized under Illinois law with its principal place of business in Cook County, Illinois.

JURISDICTION & VENUE

9. This Court has original subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because this case is brought as a putative class action pursuant to Fed. R. Civ. P. 23, at least one proposed Class member is of diverse citizenship from Defendant, the proposed

Class includes more than 100 members, and the aggregate amount in controversy exceeds $5 million.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because many of the acts and transactions giving rise to this action occurred in this District, Defendant has its principal place of business in this District, and Defendant's conduct has caused harm to Class members residing within this District.

FACTUAL ALLEGATIONS

Defendant's Promises and Obligations Regarding Protection of PII/PHI

11. IBJI is a medical company that provides healthcare services to patients.

12. Plaintiff and Class members obtained medical treatment from IBJI and were required to provide IBJI with sensitive and confidential information, including their names, dates of birth, and Social Security numbers, which is static information that does not change and can be used to commit myriad financial crimes as well as identity theft. Plaintiff and Class members also provided information, including but not limited to treatment information, health information, financial account information, and government issued identification numbers such as driver's license numbers, which information can also be used to perpetrate financial and identity crimes that severely impact the victims.

13. Plaintiff and Class members relied on Defendant, a licensed medical treatment provider, to keep their PII/PHI confidential, secure, and to use it only for purposes of treatment and billing for authorized treatment, and to implement and follow adequate and reasonable data collection, storage, and retention policies. Defendant maintained and stored the PII/PHI on its systems and networks that were inadequately protected and ultimately accessed without authorization by criminals in the Data Breach.

14. Defendant owed Plaintiff and Class members numerous statutory, regulatory, ethical, contractual, and common law duties to safeguard and keep Plaintiff's and Class members' PII/PHI confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, and theft.

15. IBJI promised Plaintiff and Class members that it "takes patient confidentiality of utmost seriousness" and acknowledges that it is "required by the State of Illinois and federal law to maintain the privacy of [their] protected health information."[2]

16. Defendant also recognized its responsibility and voluntarily adopted policies and procedures to protect PII/PHI in its Notice of Privacy Practices.[3] The Notice specifically represents that PII/PHI will be used and disclosed for purposes such as treatment, payment, and healthcare operations. Defendant further states that "other uses and disclosures of PHI not covered by [its Notice of Privacy Practices] will be made only with [the patient's] written authorization, unless otherwise permitted or required by law."[4] The Notice includes the representation that IBJI is "required by law to abide by the terms of [its] Notice of Privacy Practices."

17. IBJI's assurances proved hollow, however, as demonstrated by the Data Breach.

The Data Breach

18. IBJI's data breach notification letter states that on July 4, 2024, IBJI learned that an unauthorized third party gained access to its network. The letter does not state who informed IBJI, or how IBJI learned about the Data Breach. The letter states that the unauthorized access began on May 30, 2024, but does not provide any details as to how it knows this was the case. According to the United States Department of Health and Human Services breach portal, the Data

[2] https://www.ibji.com/patient-resources/privacy-non-discrimination-policy.
[3] https://www.ibji.com/uploads/editor/pages/2d5c89fc1c515378e8a0f3f582b6df52505181f3.pdf.
[4] *Id.*

Breach was a "Hacking/IT incident" impacting a "Network Server" and resulted in the theft of PII/PHI concerning 182,670 patients.[5]

19. Assuming that IBJI is correct that the Data Breach began on May 30, 2024, IBJI failed to detect the presence of the hackers and the vast amount of PII/PHI that was being exfiltrated from its systems for over a month. Given the length of time the Data Breach went undetected, it stands to reason that the hackers were able to satisfy themselves that they had acquired most, if not all, of the valuable PII/PHI they could. In fact, the notification letter IBJI sent to Plaintiff admits that the hackers "acquired certain files during this period." *See*, Exhibit A.

20. On or about August 30, 2024, IBJI caused notification letters to be sent to Plaintiff and Class members, and submitted a notification to the governmental authorities, regarding the Data Breach.

21. Defendant's letter admits that on or around July 4, 2024, IBJI determined that Plaintiff's PII/PHI was stolen, but provides no explanation why IBJI then waited until August 30, 2024, to attempt to notify Plaintiff and Class members. *See*, Exhibit A The letter attempts to downplay the severity of the situation by claiming without any substantiation that "we are not aware of any such data being misused." *Id*. Nevertheless, IBJI advises Plaintiff and Class members to take steps to protect themselves against "identity theft" and "fraud." *Id*.

22. Currently, the full extent of the types of sensitive personal information, the scope of the Data Breach, and the details regarding how the Data Breach was carried out are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation. However, Plaintiff and Class members are aware that the type of data set published now provides a one-stop shop for identity thieves to wreak complete havoc on their

[5] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

lives. Given the sensitivity and static nature of the information involved (such as names, Social Security numbers, and dates of birth), and the criminal targeting and theft of this information, Plaintiff and Class members have all experienced a materialized and imminent risk of identity theft.

23. Cybersecurity experts have concluded that the kind of information taken in the Data Breach "would make it possible for malicious actors to carry out phishing attacks, social engineering, or even identity theft and bank fraud."[6]

24. The PII/PHI that was exfiltrated in the Data Breach was held in unencrypted form by Defendant, and included Plaintiff's and Class members' PII/PHI.

The Data Breach Was Preventable

25. Defendant could have prevented the Data Breach by properly securing and encrypting the PII/PHI of Plaintiff and Class members, by properly training its employees to recognize and prevent cybersecurity risks, and/or by implementing and following adequate procedures to monitor and detect data breaches. Defendant's negligence in safeguarding the PII/PHI of Plaintiff and Class members was exacerbated by the repeated warnings and alerts directed to U.S. companies warning that they should protect and secure sensitive data, especially in light of the substantial increase in cyberattacks specifically targeting healthcare providers.

The Data Breach Was Foreseeable

26. The FBI has been warning healthcare providers, such as Defendant, about the threat posed by the ransomware and other threats, and to be on the lookout for attacks.

27. The United States Cybersecurity & Infrastructure Security Agency, Department of Justice, and Department of Health & Human Services issued a Joint Cybersecurity Advisory as

[6] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack.

early as on October 28, 2020, warning of an acute threat to U.S. hospitals and healthcare providers and advising them on how to "ensure that they take timely and reasonable precautions to protect their networks from these threats."[7] The Advisory details at great length the pathways of specific viruses, malware, and online threats, and lists numerous Mitigation Steps, including:

- Patch operating systems, software, and firmware as soon as manufacturers release updates;
- Check configurations for every operating system version for organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled;
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts;
- Use multi-factor authentication where possible;
- Disable unused remote access/remote desktop protocol (RDP) ports and monitor remote access/RDP logs;
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy;
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind;
- Audit logs to ensure new accounts are legitimate;
- Scan for open or listening ports and mediate those that are not needed;

[7] https://www.cisa.gov/uscert/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.

- Identify critical assets such as potential database servers, medical records, and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network;
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment;
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

28. In addition, the advisory emphasizes a focus on awareness and training. Because end users are targeted, employees need to be aware of threats and how they are delivered.

29. On information and belief, the hackers who carried out the Data Breach used rudimentary tactics for deploying malware on data rich systems, such as basic phishing emails. Such attacks are entirely preventable through proper training of employees to recognize phishing emails in combination with industry standard security measures such as required two-factor or multi-factor authentication to access email accounts and/or other computer systems.

30. Even with a successful initial infection vector through basic phishing techniques, the Data Breach could have been identified and halted quickly had Defendant implemented widely available software capable of fully detecting and preventing the Data Breach. However, due to the lack of such protective measures, the Data Breach went undetected for over a month.

31. Despite the well-known risks and reasonable and effective protections, Defendant inexplicably failed to properly train employees, failed to implement industry standard security measures, and maintained highly sensitive patient information in a manner it knew or should have known was vulnerable to access and exfiltration.

32. Despite the prevalence of public announcements of these data breach and data security compromises and despite numerous attempts on the part of the federal government to inform healthcare providers, like Defendant, of the threats facing Defendant, and despite having ample time to implement precautions and training, Defendant was negligent and did not adequately prepare for this wholly foreseeable event; thus, allowing extremely sensitive data to be accessed, viewed and stolen by the criminals. Defendant breached its duty to take appropriate steps to protect Plaintiff's and Class members' PII/PHI from being compromised and failed to adequately notify them that the Data Breach took place.

33. Unfortunately for Plaintiff and Class members, their PII/PHI was not secured in the manner required by law that would have prevented the Data Breach.

34. What is worse, despite Defendant's obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendant failed to promptly provide such notice in the most expedient time possible and without unreasonable delay, failed to include in the Data Breach notification letter a sufficient description of the Data Breach or the information needed by Plaintiff and Class members to react appropriately to the Data Breach, including taking whatever mitigation measures are necessary.

35. As a result, this unauthorized access, disclosure, and exfiltration remains unremedied, and as detailed below the "cure" offered by Defendant to address these failures after the fact was wholly inadequate.

36. Defendant had specific obligations imposed on it by contracts and law to ensure the adequate protection of such information. For example, as a covered entity under HIPAA, Defendant was required to maintain the confidentiality and security of the PII/PHI of its patients.

Defendant's HIPAA Violations

37. Defendant is regulated by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102), and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendant's protection of medical information maintained in electronic form.

38. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

39. "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

40. HIPAA's Security Rule requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by its workforce.

41. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and also to "[i]mplement

technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

42. The facts of the Data Breach establish that Defendant failed to comply with these Rules. The Data Breach resulted from a combination of inadequacies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

(j) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

Defendant Violated Federal Trade Commission Guidelines

43. Defendant also violated the duties applicable to it under the Federal Trade Commission Act (15 U.S.C. § 45, *et seq*.) from engaging in "unfair or deceptive acts or practices

in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

44. As established by these laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the medical information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant also owed a duty to Plaintiff and Class members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that its computer systems, networks, and protocols adequately protected this medical information and were not exposed to infiltration. This also included a duty to Plaintiff and Class members to design, maintain, and test its computer systems to ensure that the PII/PHI was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the PII/PHI through processes such as phishing, including adequately training employees and others who accessed information within its systems on how to adequately protect this information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of its data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft; and to disclose in a timely and accurate manner when data breaches occurred.

45. Defendant also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems. It is apparent that Defendant did not do so.

46. Defendant owed these duties to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendant affirmatively chose to design these systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in criminals successfully carrying out a cyberattack and exfiltrating Plaintiff's and Class members' PII/PHI, to the injury and detriment of Plaintiff and Class members. By taking affirmative acts inconsistent with these obligations that left Defendant's computer systems foreseeably vulnerable to criminals, Defendant disclosed and/or permitted the disclosure of PII/PHI to unauthorized third parties. Defendant thus failed to preserve the confidentiality of PII/PHI it was duty-bound to protect.

Value of Personally Identifiable Information

47. The PII/PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

48. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an

[8] https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[9] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[10]

49. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

50. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[11]

51. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

52. Indeed, a robust cyber black market exists in which criminals post stolen medical information, PII/PHI on multiple underground internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access

[10] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[11] http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

prescriptions for illegal use or resale. According to a 2017 Javelin strategy and research presentation, fraudulent activities based on data stolen in data breaches that are between two and six years old had increased by nearly 400% over the previous four years.[12] Thus, an offer of credit monitoring service that is only for two years is not an adequate remedy or offer, even if it conducts dark web scanning (which is unclear here).

53. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[13] PII/PHI can be sold at a price ranging from approximately $20 to $300.[14]

54. In this case, all evidence indicates that Plaintiff and Class members' PII/PHI was left unprotected, to be exfiltrated and sold on the dark web. Thus, this highly valuable data was left to be pilfered by criminals or reviewed by anyone with an Internet connection.

55. Medical identity theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences since if a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[15]

[12] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.
[13] *Id.*
[14] https://www.privacyaffairs.com/dark-web-price-index-2021.
[15] https://khn.org/news/rise-of-indentity-theft; *see also*, https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare.

56. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to resolve the breach.[16]

57. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[17]

58. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security numbers and names, is impossible to "close" and difficult, if not impossible, to change.

59. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

60. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

61. The fraudulent activity resulting from the Data Breach may not come to light for years.

[16] https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.
[17] http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.
[18] https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

62. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

63. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII/PHI of Plaintiff and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

64. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII/PHI.

65. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

66. To date, Defendant has offered Plaintiff and Class members only one year of identity theft detection services. The offered service is wholly inadequate to protect Plaintiff and

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov /assets/gao-07-737.pdf.

Class members from the threats they face for years to come, particularly in light of the PII/PHI at issue here, and is not an adequate cure of the Data Breach.

67. Specifically, Defendant has not and cannot retrieve the PII/PHI taken from its systems. Thus, Plaintiff's and Class members' PII/PHI will remain in circulation on the Internet for access, viewing, and misuse, causing damage to Plaintiff and Class members and breaching their confidentiality.

68. Defendant has not provided sufficient information in its Data Breach notice letter such that Plaintiff and Class members could understand and appreciate the full nature of the risk to them caused by Defendant's Data Breach, allowing them to make informed decisions about how to protect themselves and their PII/PHI.

69. Defendant has not provided credit monitoring and identity theft protection to Plaintiff and Class members for a long enough period of time, limiting the bulk of the protection services to one year even though their PII/PHI may be used for years after that.

70. Defendant's identity theft protection offer of Experian's IdentityWorks Credit 3B does not prevent fraudulent transactions, such as unauthorized credit card charges or exchanges of Plaintiff's PII/PHI on the dark web from occurring using the PII/PHI disclosed by Defendant. Further, IdentityWorks Credit 3B does not provide 3-Bureau Credit Report & FICO Scores monthly, unlike other Experian products.

71. Enrollment in IdentityWorks Credit 3B requires Plaintiff and Class members to disclose PII/PHI to Experian, a company that had its own data breach in 2015 exposing the personal information of approximately 15 million individuals.

72. Additionally, Defendant has not taken the actions necessary and recommended by the FBI, CISA, NSA and other experts detailed above to prevent an attack by criminals, leaving Plaintiff and Class members vulnerable to subsequent breaches of their PII/PHI held by Defendant.

73. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII/PHI of Plaintiff and Class members.

PLAINTIFF'S EXPERIENCES

74. Plaintiff received healthcare from Defendant in approximately spring of 2022. As a condition of obtaining treatment, Plaintiff provided PII/PHI to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use her PII/PHI for legitimate business purposes.

75. Defendant expressly and impliedly promised to safeguard Plaintiff's PII/PHI. Defendant assumed obligations to Plaintiff, and Plaintiff relied on Defendant to safeguard her PII/PHI and only to utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiff's PII/PHI, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies. Had Plaintiff known her PII/PHI would be insufficiently protected from known cyberthreats, Plaintiff would not have disclosed the information to Defendant and would not have paid as much as she did for the healthcare services she bargained to receive—of which confidentiality was a material term.

76. On or about August 30, 2024, Plaintiff received notice from Defendant that her PII/PHI had been improperly accessed and/or obtained by unauthorized third parties. *See*, Exhibit A. This notice indicated that Plaintiff's PII/PHI, including her name, address, date of birth, Social

Security number, driver's license number, medical treatment or diagnosis information, and health insurance or claims information was compromised as a result of the Data Breach.

77. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; and reviewing financial, healthcare, and other accounts for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work or recreation

78. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of her PII/PHI, which she reasonably believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her PII/PHI for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

79. Plaintiff suffered actual injury from having her PII/PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII/PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; (c) loss of the benefit of her bargained-for data security protections; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

80. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

81. Plaintiff seeks to certify the following Class of similarly situated persons under Fed. R. Civ. P. 23:

> All individuals whose PII/PHI was contained on the files obtained by unauthorized third parties in the Data Breach.

82. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their immediate families and members of their staff.

83. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

84. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, Plaintiff believes that the Class may consist of approximately 182,670 persons based on Defendant's report to the Department of Health & Human Services.[20]

85. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

(a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' PII/PHI;

[20] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

(b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(c) Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

(d) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

(e) Whether Defendant owed a duty to Class members to safeguard their PII/PHI;

(f) Whether Defendant breached its duty to Class members to safeguard their PII/PHI;

(g) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

(h) Whether Defendant should have discovered the Data Breach sooner;

(i) Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

(j) Whether Defendant's conduct was negligent;

(k) Whether Defendant's acts, inactions, and practices complained of herein breached express or implied contracts with Plaintiff and Class members;

(l) Whether Defendant breached a fiduciary duty and duties of confidentiality to Plaintiff and Class members;

(m) Whether Defendant violated the Personal Information Protection Act;

(n) Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class members; and

(o) Whether Plaintiff and Class members are entitled to damages, punitive damages, treble damages, and/or injunctive or other equitable relief.

86. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was compromised in the Data Breach.

87. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel is competent and experienced in litigating class actions.

88. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that all of Plaintiff's and Class members' PII/PHI was stored on the same computer network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

89. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for

Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

90. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(on behalf of Plaintiff and the Class)

91. Plaintiff re-alleges and incorporates by reference all of the allegations in paragraphs 1-90 of the Complaint as if fully set forth herein.

92. As a condition of obtaining treatment, Plaintiff and Class members provided Defendant with their PII/PHI.

93. Plaintiff and Class members entrusted their PII/PHI to Defendant with the understanding and reliance upon Defendant to exercise reasonable care in the protection of their PII/PHI.

94. Defendant had a duty to take reasonable measures to protect the PII/PHI of Plaintiff and Class members from unauthorized disclosure to third parties. This duty is inherent in the nature of the exchange of highly sensitive personal information in connection with the patient-physician relationship.

95. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and Class members could and would suffer if the PII/PHI were wrongfully disclosed in a Data Breach.

96. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, using, and retaining of the PII/PHI of Plaintiff and Class members, without adequate data security, involved an unreasonable risk of harm to Plaintiff and Class members.

97. Defendant had a duty to exercise reasonable care in safeguarding, securing, retaining, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, design, configuring, maintaining, and testing Defendant's security protocols to ensure that the PII/PHI of Plaintiff and Class members in Defendant's possession was adequately secured and protected.

98. Defendant also had a duty to exercise appropriate practices to remove PII/PHI that was no longer required.

99. Defendant had a duty to encrypt the sensitive PII/PHI it stored and maintained.

100. Defendant had a duty to segregate sensitive PII/PHI from other portions of its network, such as by using firewalls.

101. Defendant had a duty to properly train employees to recognize phishing attempts and other common data security risks.

102. Defendant also had a duty to implement and maintain procedures to detect and prevent the improper access, exfiltration, and misuse of PII/PHI.

103. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiff and Class members. Plaintiff and Class members entrusted Defendant with their confidential PII/PHI and relied upon Defendant to implement adequate data security and reasonable data retention policies.

104. Defendant was subject to an independent duty untethered to any contract between Defendant and Plaintiff or Class members.

105. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, the detailed warnings published by governmental agencies, and news reports of other data breaches.

106. Plaintiff and Class members were the foreseeable and probable victims of Defendant's inadequate and unreasonable data security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII/PHI, the critical importance of providing adequate security of that PII/PHI, the necessity for encrypting PII/PHI, and the harm that can arise from retaining PII/PHI following the expiration of any legitimate business purpose.

107. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant solicited, collected, digitized, and aggregated Plaintiff's and Class members' PII/PHI, failed to encrypt the PII/PHI, failed to implement other reasonable industry standard measures to safeguard PII/PHI, and failed to implement retention policies that delete PII/PHI.

108. Plaintiff and Class members had no ability to protect their PII/PHI that was in, and remains in, Defendant's possession, and no sign that Defendant was failing and refusing to implement and maintain reasonable data security practices over their PII/PHI until they received their notification letters.

109. Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

110. Defendant had and continues to have a duty to adequately disclose that the PII/PHI might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and the Class members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII/PHI.

111. Defendant had a duty to employ proper procedures to prevent the unauthorized disclosure and unauthorized sharing of the PII/PHI to criminals.

112. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class members by failing to implement and maintain industry-standard protocols and to exercise reasonable care in protecting and safeguarding the PII/PHI of Plaintiff and Class members.

113. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and Class members in violation of standard industry rules, regulations, and practices at the time of the Data Breach.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of PII/PHI.

115. Defendant breached its duty to remove PII/PHI that it was no longer required to retain pursuant to regulations.

116. Defendant breached its duty to encrypt PII/PHI and to segregate it from other portions of its network.

117. Defendant breached its duty to adequately train employees to recognize and avoid phishing attempts and other basic cybersecurity risks.

118. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class members the existence and scope of the Data Breach.

119. Defendant breached its duty to safeguard Plaintiff's and Class members' PII/PHI by failing to retain such information in an encrypted form.

120. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the PII/PHI of Plaintiff and Class members would not have been compromised.

121. There is a close causal connection between Defendant's failure to implement security measures to protect the PII/PHI of Plaintiff and Class members and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. The PII/PHI of Plaintiff and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

122. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiff and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

123. As Defendant instructed, advised, and warned in its notice letters, Plaintiff and Class members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included, and will include into the future, protective steps: *e.g.*, reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other

mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

124. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiff and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their PII/PHI.

125. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession. Plaintiff and Class members are, therefore, also seeking injunctive relief for the continued risk to their PII/PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the PII/PHI.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to recover actual and punitive damages.

COUNT II
Negligence *per se*
(on behalf of Plaintiff and the Class)

127. Plaintiff re-alleges and incorporates by reference all of the allegations in paragraphs 1-90 of the Complaint as if fully set forth herein.

128. Defendant violated HIPAA regulations, including by:

- Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. section 164.306(a)(1);
- Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);
- Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);
- Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);
- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

- Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);
- Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);
- Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;
- Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and
- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

129. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United

States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One*, 488 F. Supp. 3d at 407.

130. Plaintiff's and Class members' PII/PHI was and is nonpublic personal information and customer information.

131. Plaintiff and Class members are in the group of persons that HIPAA and the FTC Act were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendant's violations of HIPAA and the FTC Act were the types of harm the statutes and regulations are designed to prevent.

132. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiff and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

133. As a direct and proximate result of the conduct of Defendant that violated HIPAA and the FTC Act, Plaintiff and Class members have suffered and will continue to suffer the foreseeable economic and non-economic harms as described herein.

134. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to recover actual and punitive damages.

COUNT III
Breach of Implied Contract
(on behalf of Plaintiff and the Class)

135. Plaintiff re-alleges and incorporates by reference all of the allegations in paragraphs 1-90 of the Complaint as if fully set forth herein.

136. Defendant required Plaintiff and Class members to provide their PII/PHI as a condition of receiving treatment. In so doing, Plaintiff and Class members entered into implied

contracts with Defendant wherein Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class members if their PII/PHI had been breached and compromised or stolen.

137. Defendant further entered into an implied contract with Plaintiff and the Class members to honor its representations and assurances regarding protecting their PII/PHI.

138. Plaintiff and Class members fully performed their obligations under implied contracts with Defendant.

139. Defendant breached the implied contracts it made with Plaintiff and Class members by (i) failing to implement technical, administrative, and physical security measures to protect the PII/PHI from unauthorized access or disclosure (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the PII/PHI to those with legitimate reasons to access it, (iii) failing to store the PII/PHI only on servers kept in a secure, restricted area, and (iv) otherwise failing to safeguard the PII/PHI.

140. As a direct and proximate result of Defendant's breach of its implied contract, Plaintiff and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

141. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (d) financial costs incurred

due to actual identity theft; (e) the cost of future identity theft monitoring; (f) loss of time incurred due to actual identity theft; (g) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls, (h) failure to receive the benefit of their bargained for data protection for which Plaintiff and Class members paid a premium to Defendant; and (i) diminution of value of their PII/PHI.

142. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
Violation of Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.
(on behalf of Plaintiff and the Class)

143. Plaintiff re-alleges and incorporates by reference all of allegations in paragraphs 1-90 of the Complaint as if fully set forth herein.

144. As a business that collects, handles, stores, and maintains patient information that is nonpublic and personally identifiable information, Defendant is a data collector within the meaning of 815 ILCS 530/5.

145. As a data collector, Defendant is required to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII/PHI from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45.

146. Defendant breached these duties and the applicable standards of care by:

- Failing to conduct proper and reasonable due diligence and oversight over employees, agents, and vendors who access to PII/PHI and their data security systems, practices, and procedures;

- Failing to conduct proper and reasonable due diligence over the employees, agents, and vendors who were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and Class members';
- Failing to maintain reasonable and appropriate oversight and audits on employees, agents, or vendors who were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and Class members' PII/PHI;
- Failing to implement and maintain reasonable safeguards and procedures, such as encryption, to prevent the unauthorized disclosure of Plaintiff's and Class members' PII/PHI;
- Failing to monitor and detect its confidential and sensitive data environment(s) storing Plaintiff's and Class members' PII/PHI reasonably and appropriately in order to repel or limit the Data Breach;
- Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII/PHI to ensure the PII/PHI was being stored and maintained for legitimate and useful purposes;
- Failing to undertake reasonable and sufficient incident response measures to ensure that the cyberattack directed toward Defendant's sensitive information would be thwarted and not expose and cause disclosure and unauthorized acquisition of Plaintiff's and Class members' PII/PHI;
- Failing to cure deficiencies in data security that allowed the Data Breach to continue, grow in severity and scope, and go undetected and undeterred for additional time;

- Failing to ensure that Plaintiff's and Class members' PII/PHI was timely deleted, destroyed, rendered unable to be used, or returned to Plaintiff and Class members;
- Failing to reasonably conduct a forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;
- Failing to provide full disclosure about, and deceptively misleading consumers through false representations and misleading omissions of fact regarding, the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and
- Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII/PHI, and details regarding the disposition of Plaintiff's and the other Class members' PII/PHI at all times during the Data Breach.

147. Defendant failed to timely notify Plaintiff and Class members that their PII/PHI was acquired in the Data Breach. Defendant waited 57 days to mail a letter to Plaintiff and Class members. Defendant had all the information it needed to disseminate notification to Plaintiff and the other Class members on July 4, 2024, when it learned of the Data Breach. Likely, notification could have been provided in mere days to all the individuals whose names and information was contained in the files that were accessed by the criminals. Instead, Defendant delayed notification while cyber criminals were able to perpetrate fraud with Plaintiff's and Class members' PII/PHI

unbeknownst to them for an additional two months after Defendant became aware of the Data Breach.

148. As a proximate result of Defendant's unfair acts and practices described above and the resulting injuries to Plaintiff and Class members, as herein alleged, Plaintiff and Class members have incurred damages.

149. As a direct and proximate result of Defendant's unlawful acts and omissions, Plaintiff and Class members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their PII/PHI.

150. Additionally, as a direct and proximate result of Defendant's unlawful conduct, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession. Plaintiff and Class members are, therefore, also seeking injunctive relief for the continued risk to their PII/PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the PII/PHI.

151. As a direct and proximate result of Defendant's unlawful conduct, Plaintiff and Class members are entitled to recover actual, consequential, punitive damages, as well as injunctive relief, and reasonable attorney's fees and costs, pursuant to 815 ILCS 505/10a and 815 ILCS 505/2z.

COUNT V
Unjust Enrichment
(on behalf of Plaintiff and the Class)

152. Plaintiff re-alleges and incorporates by reference all of the allegations in paragraphs 1-90 of the Complaint as if fully set forth herein.

153. This claim is brought in the alternative to Plaintiff's other claims at law.

154. Defendant benefited from receiving Plaintiff's and Class members' PII/PHI by its ability to retain and use that information for its own benefit.

155. Defendant also understood and appreciated that Plaintiff's and Class members' PII/PHI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

156. Plaintiff and Class members conferred a benefit upon Defendant by paying for its services, and in connection therewith, by providing their PII/PHI to Defendant with the understanding that Defendant would implement and maintain reasonable data privacy and security practices and procedures. Plaintiff and Class members should have received adequate protection and data security for such PII/PHI held by Defendant.

157. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and appreciated the benefits.

158. Defendant failed to provide reasonable security, safeguards, and protections to the PII/PHI of Plaintiff and Class members.

159. Defendant should not be permitted to retain money rightfully belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data security measures and caused the Data Breach.

160. Defendant accepted and wrongfully retained these benefits to the detriment of Plaintiff and Class members.

161. Defendant's enrichment at the expense of Plaintiff and Class members is and was unjust.

162. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and Class members seek restitution of their money paid to Defendant, and disgorgement of all profits, benefits, imposition of a constructive trust, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for judgment against Defendant and in Plaintiff's favor, as follows:

(a) For an Order certifying this action as a Class action, and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

(b) For an award of actual damages, compensatory damages, nominal damages, consequential damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

(c) For an award of punitive damages, as allowable by law

(d) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII/PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

(e) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

(f) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

(g) Imposition of a constructive trust for the benefit of Plaintiff and Class members;

(h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

(i) Pre- and post-judgment interest on any amounts awarded; and,

(j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Plaintiff ALEXANDRA PHELPS, individually, and on behalf of all others similarly situated,

By: /s/ Thomas A. Zimmerman, Jr.

Thomas A. Zimmerman, Jr. (IL #6231944)
tom@attorneyzim.com
Sharon A. Harris
sharon@attorneyzim.com
Matthew C. De Re
matt@attorneyzim.com
Jeffrey D. Blake
jeff@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Tel: (312) 440-0020
Fax: (312) 440-4180
www.attorneyzim.com

Counsel for Plaintiff and the Putative Class

ILLINOIS BONE & JOINT INSTITUTE®

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Alexandra Phelps
[redacted]
147526

August 30, 2024

RE: NOTICE OF DATA BREACH

Dear Alexandra Phelps:

Illinois Bone & Joint Institute, LLC ("IBJI") values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. Importantly, we remained open and continued to treat IBJI patients throughout this incident. This letter explains the incident, the steps we have taken in response, and provides information on steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? On July 4, 2024, we detected unauthorized access to certain computer systems on the IBJI network. We immediately initiated an investigation, retained cybersecurity experts, and notified law enforcement. Through its IT infrastructure, IBJI took all steps to immediately secure its environment from any additional malicious activities in order to safeguard its systems. The investigation determined that an unauthorized third party accessed the IBJI network between May 30, 2024, and July 4, 2024, and acquired certain files during this period. To date, we are not aware of any such data being misused.

What Information Was Involved? Based on the results of our thorough investigation, we reviewed the affected systems to identify the individuals whose information may have been accessed or acquired without authorization during the incident. We have since determined that the systems may contain personal information that included your name, address, date of birth, Social Security number, medical treatment or diagnosis information, and health insurance or claims information.

What We Are Doing. In addition to the actions described above, we are taking steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft involving your information, we are also offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* sheet.

EXHIBIT A